VIT
Vellore Institute of Technology

REG.NO.:

SLOT: B2+TB2

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - I
WINTER SEMESTER 2025-2026

Expansion Permutation (E)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

S Box (S1 Table)

S1

Column Number

Row No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

4.	In AES encryption algorithm, the SubBytes operation is applied to the state matrix using the AES S-Box. After the SubBytes step of a particular AES round, the following 4 × 4 state matrix (in hexadecimal) is obtained: D4 E0 B8 1E 27 BF B4 41 11 98 5D 52 AE F1 E5 30 The AES MixColumns transformation uses the following fixed matrix defined over GF(2^8): 02 03 01 01 01 02 03 01 01 01 02 03 03 01 01 02 a. Apply the ShiftRows transformation and write the resulting state matrix.	2		2	4
	b. Apply the MixColumns transformation on the entire state matrix obtained in part a. Provide the detailed calculations with all the steps for the **first column** only		7		
5.	Consider the RC4 stream cipher with a reduced state size N = 8. Initial permutation array: S = [0, 1, 2, 3, 4, 5, 6, 7] Key array: K = [1, 2, 4, 3] Perform the Key Scheduling Algorithm (KSA) for the given key and compute the final permutation array S after completing all 8 iterations. Show the value of i, j, swaps performed, and the S array at each step.	2	10	2	4

REG.NO.: 23BCT0001

SLOT: B2+TB2

VIT

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - I
WINTER SEMESTER 2025-2026

Programme Name & Branch : B. Tech CSE and All Specialization
Course Code and Course Name : BCSE309L_ Cryptography and Network Security
Faculty Name(s) : COMMON TO ALL
Class Number(s) : COMMON TO ALL
Date of Examination : 28-Jan-2026
Exam Duration : 90 minutes
Maximum Marks: 50

General instruction(s):

- Answer All Questions
- M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)
- Course Outcomes

1. To know the fundamental mathematical concepts related to security.
2. To understand concept of various cryptographic techniques.

Q. No	Question	Module	Marks	CO	BL
1.	a. State the steps of Extended Euclidean algorithm and also find the values of x and y for a=428 and b=1215.	1	5	1	3
	b. Using Fermat's theorem and Fast Modular Exponentiation method, find 7^{181} mod 31		5		
2.	a. Define Group and Ring. Prove Z_7 is a Ring or not.	1	5	1	2
	b. Solve for X using the Chinese Remainder Theorem (CRT) $X \equiv 3 \bmod 5$ $X \equiv 4 \bmod 7$ $X \equiv 5 \bmod 9$		5		
3.	Given a 64-bit block sequence, perform the following operations using the DES algorithm. Use the tables for your reference. Block sequence: 7A94C2E1 (Each hexadecimal digit represents 4 bits → 8 × 4 = 32 bits) Subkey: 3B2F91A6C4D8 (12 hexadecimal digits → 12 × 4 = 48 bits) a) Expansion using P-box (3 Marks) b) XOR with the given subkey (2 Marks) c) Take the output achieved from Part b and compute the output of S-box S1. Show the row selection, column selection, and the resulting 4-bit value in both decimal and binary (5 Marks)	2	10	2	3